

Application No. 09/923,075
Response dated November 14, 2005
Reply to Office Action of July 14, 2005
Page 5 of 7

REMARKS

The Office Action has been carefully reviewed. The following remarks herein are considered responsive thereto. Within this response claims 1—11 have been withdrawn, claim 12 has been amended, and claims 21—29 have been added. Claims 12—29 are currently pending in the application.

INFORMATION DISCLOSURE STATEMENT

In the July 14, 2005, Office Action, the Examiner requested that the Applicant specify which prior art as cited on the previously submitted PTO-1449 forms have particular relevancy to the patentability of the presently claimed invention.

In response to the Examiner's request, the Applicant would respectfully turn the Examiner's attention to the information disclosure statement as filed by the Applicant on August 14, 2003. The Applicant would respectfully specify that the Examiner consider citations nos. 24 and 31—33 as being of particular pertinence to the presently pending application. Applicant is currently not aware of any additional citations that comprise any significant relevance to the presently pending patent application.

REJECTIONS AS TO SUBSTANCE

In the Office Action of July 14, 2005, the Examiner rejected claims 12—14 under 35 U.S.C. § 101. Claims 12 and 15—17 were rejected under 35 U.S.C. § 102(b) as being anticipated by Federal Information Processing Standards Publication 186 (FIPS 186). Claim 13 was rejected under 35 U.S.C. § 103(a) as being unpatentable over FIPS 186 in view of U.S. Patent No. 6,775,772 issued to Binding. Claim 14 was rejected under 35 U.S.C. § 103(a) as being unpatentable over FIPS 186 in view of U.S. Patent No. 6,073,237 issued to Ellison. Claim 18, was rejected under 35 U.S.C. § 103(a) as being unpatentable over FIPS 186 in view of Applicant's admitted prior art. Lastly, claims 19 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over FIPS 186 in view of U.S. Patent No. 6,594,759 issued to Wang.

Currently, independent claim 12 has been amended and independent claim 21 and

Application No. 09/923,075
Response dated November 14, 2005
Reply to Office Action of July 14, 2005
Page 6 of 7

dependent claims 22—29 have been added. Independent claims 12 and 21 recite limitations that are directed to the generation of a digital signature for use as a random number for utilization in an application that requires a random number. Further, both claims recite limitations directed to generating at a device a digital signature using a digital signature algorithm and using the generated digital signature as the random number in an application that is external to the device.

Support for the presently claimed amendments can be found at page 17, lines 20 – 24, and page 40, line 36 – page 41, line 18. No new matter has been added by this amendment.

As per the rejection of claims 12—14 under 35 U.S.C. § 101, as being directed to non-statutory subject matter, as referenced above, independent claim 12 has been amended to recite limitations that are directed to a new and useful process. In light of the amendments to claim 12, the Applicant respectfully requests that the rejection of claims 12 – 14 under 35 U.S.C. § 101 be withdrawn.

In regard to claim 12, the Examiner has cited FIPS 186 for disclosing a digital signature algorithm (DSA), wherein the digital signature is generated by a sender, the digital signature being a random number.

Specifically, FIPS 186 describes a suite of algorithms that are used to generate a digital signature. Moreover, the digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use the digital signature in proving to a third party that the signatory in fact generated the signature.

In contrast to the presently claimed invention, FIPS 186 does not disclose or describe a system or method wherein a private key of a public/private key pair is stored within a device in addition to the generation of a digital signature within the device and thereafter using the generated digital signature as the random number in an application that is external to the device. Nowhere in FIPS 186 are specific structures described wherein digital signatures may be generated. Specifically, FIPS 186 merely describes problem-solving procedures for generating digital signatures, nowhere in FIPS 186 is described or

Application No. 09/923,075
Response dated November 14, 2005
Reply to Office Action of July 14, 2005
Page 7 of 7

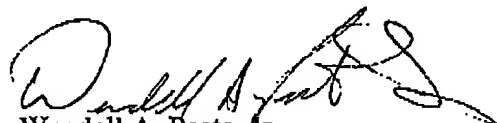
disclosed any devices or methods for using devices to accomplish the objectives of FIPS 186.

Thus, FIPS 186 does not describe or disclose storing a private key of a public/private key pair within a device and generating a digital signature at a device and thereafter using the generated digital signature as the random number in an application that is external to the device. Therefore, in view of the fore-mentioned argument, the Applicant respectfully requests that the rejection of independent claim 12 under 35 U.S.C. § 102 (b) be withdrawn.

In view of the foregoing remarks, Applicant submits that the present claims stand in condition for allowance, and Applicant respectfully requests notice of the same. It furthermore is respectfully requested that the Examiner contact the undersigned if any further action is deemed necessary in order to gain allowance of the present application, and if such further action may be accomplished through action by the Examiner.

Respectfully submitted,

Morris, Manning & Martin, LLP



Wendell A. Peete, Jr.
Registration No. 52,108
Tel.: 404.495.3682